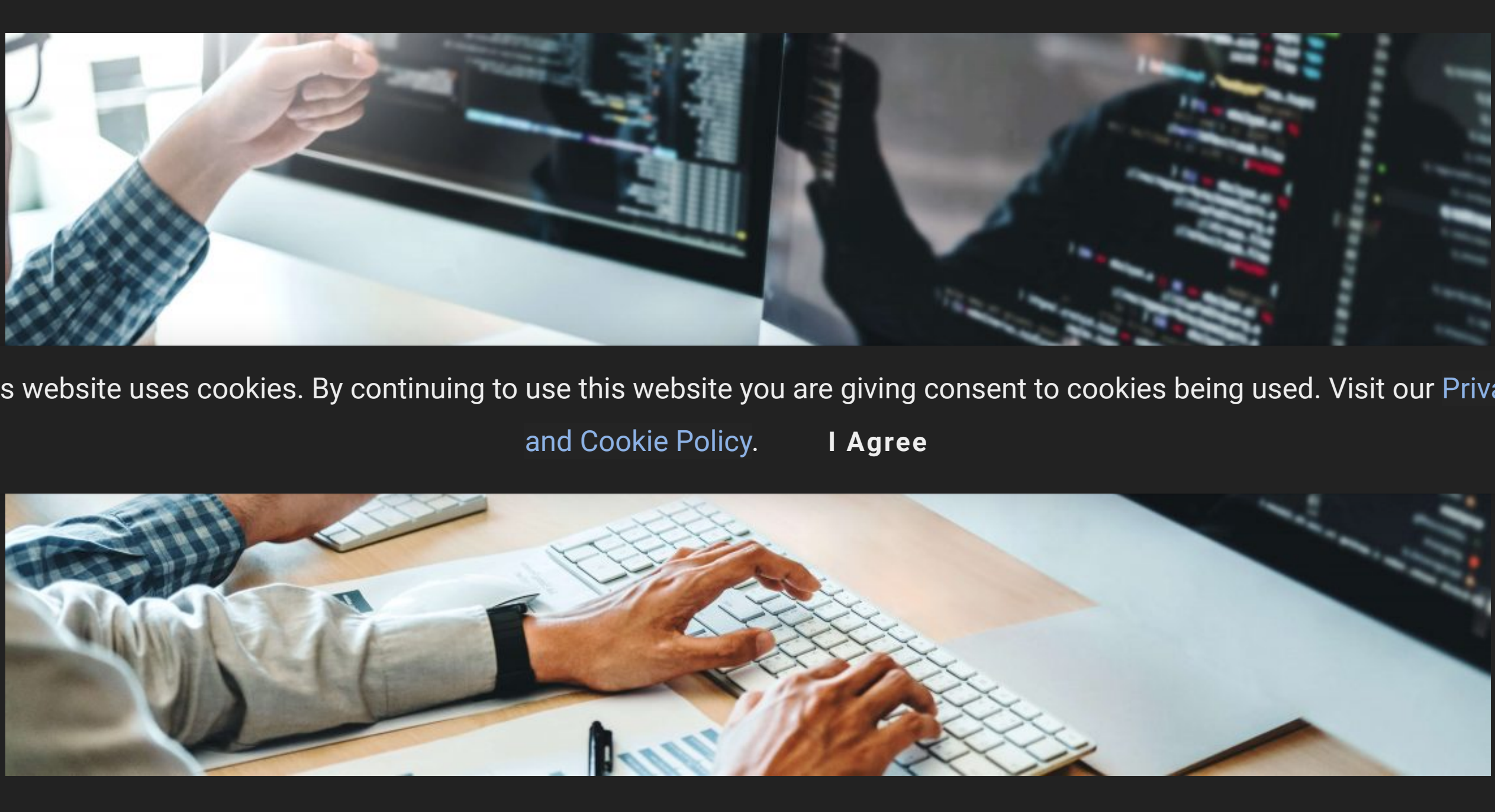
Report: unidentified database exposes 200 million Americans

by CyberNews Team — March 20, 2020 in Security 💬 1



This website uses cookies. By continuing to use this website you are giving consent to cookies being used. Visit our Privacy and Cookie Policy. **I Agree**

70 SHARES / Share on Facebook Share on Twitter

The CyberNews research team uncovered an unsecured database owned by an unidentified party, comprising **800 gigabytes of personal user information**.The database in question was left on a publicly accessible server and contained **more than 200 million detailed user records**, putting an astonishing number of people at risk.

On March 3, 2020, the entirety of the data present on the database was wiped by an unidentified party.

What was in the database?

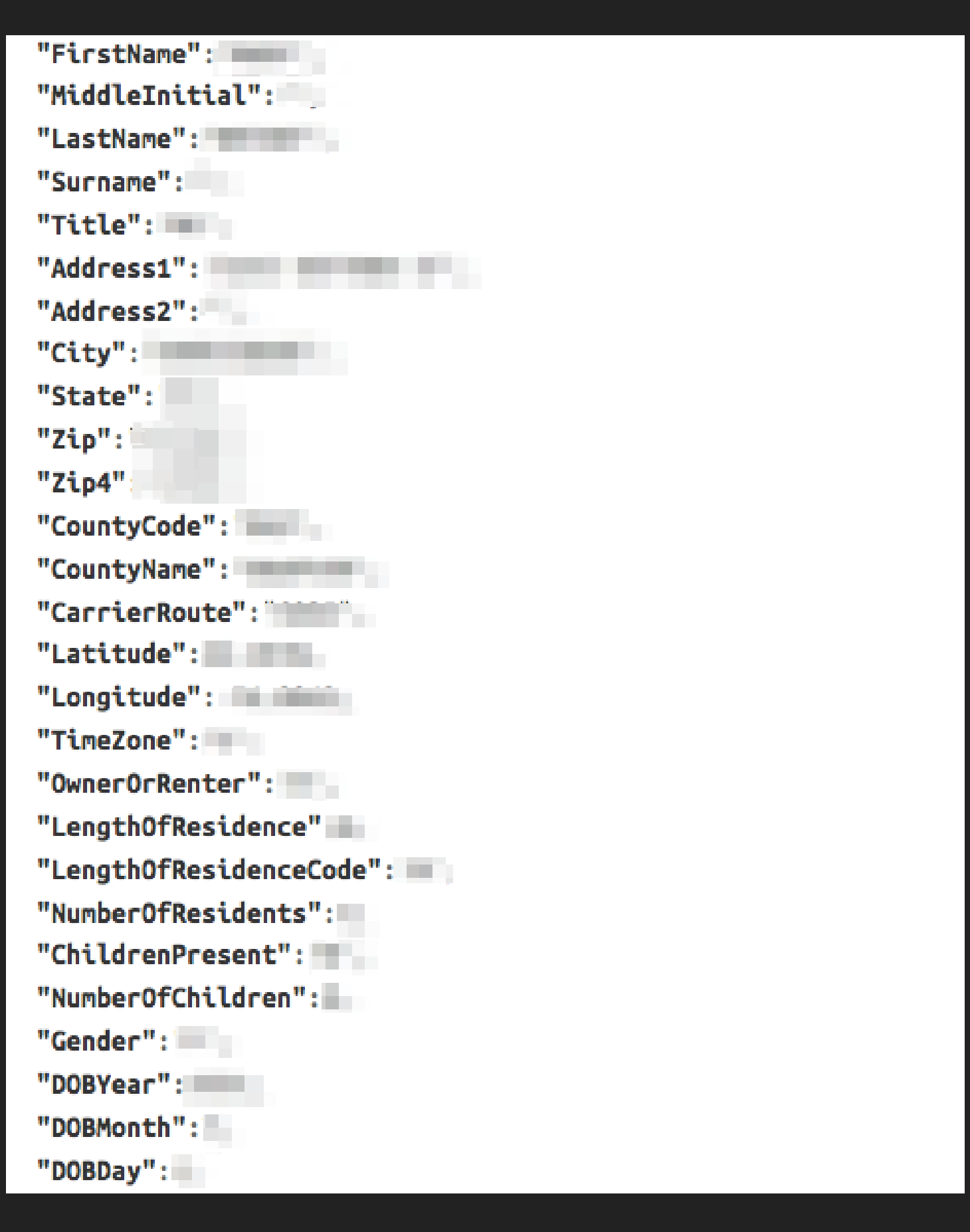
The unsecured database contained a folder that included more than 200 million incredibly detailed records of what looked like profiles of US users.

Click HERE to see if your data has been leaked.

The records contained, among other things:

- Full names and titles of the exposed individuals
- Email addresses
- Phone numbers
- Dates of birth
- Credit ratings
- Home and mortgaged real estate addresses, including their exact locations
- Demographics, including numbers of children and their genders
- Detailed mortgage and tax records
- Detailed data profiles, including information about the individuals' personal interests, investments, as well as political, charitable, and religious donations

Example of leaked records:



```
"FirstName":[redacted]
"MiddleInitial":[redacted]
"LastName":[redacted]
"Surname":[redacted]
"Title":[redacted]
"Address1":[redacted]
"Address2":[redacted]
"City":[redacted]
"State":[redacted]
"Zip":[redacted]
"Zip4"
"CountyCode":[redacted]
"CountyName":[redacted]
"CarrierRoute":[redacted]
"Latitude":[redacted]
"Longitude":[redacted]
"TimeZone":[redacted]
"OwnerOrRenter":[redacted]
"LengthOfResidence"[redacted]
"LengthOfResidenceCode":[redacted]
"NumberOfResidents":[redacted]
"ChildrenPresent":[redacted]
"NumberOfChildren":[redacted]
"Gender":[redacted]
"DOBYear":[redacted]
"DOBMonth":[redacted]
"DOBDay":[redacted]
```

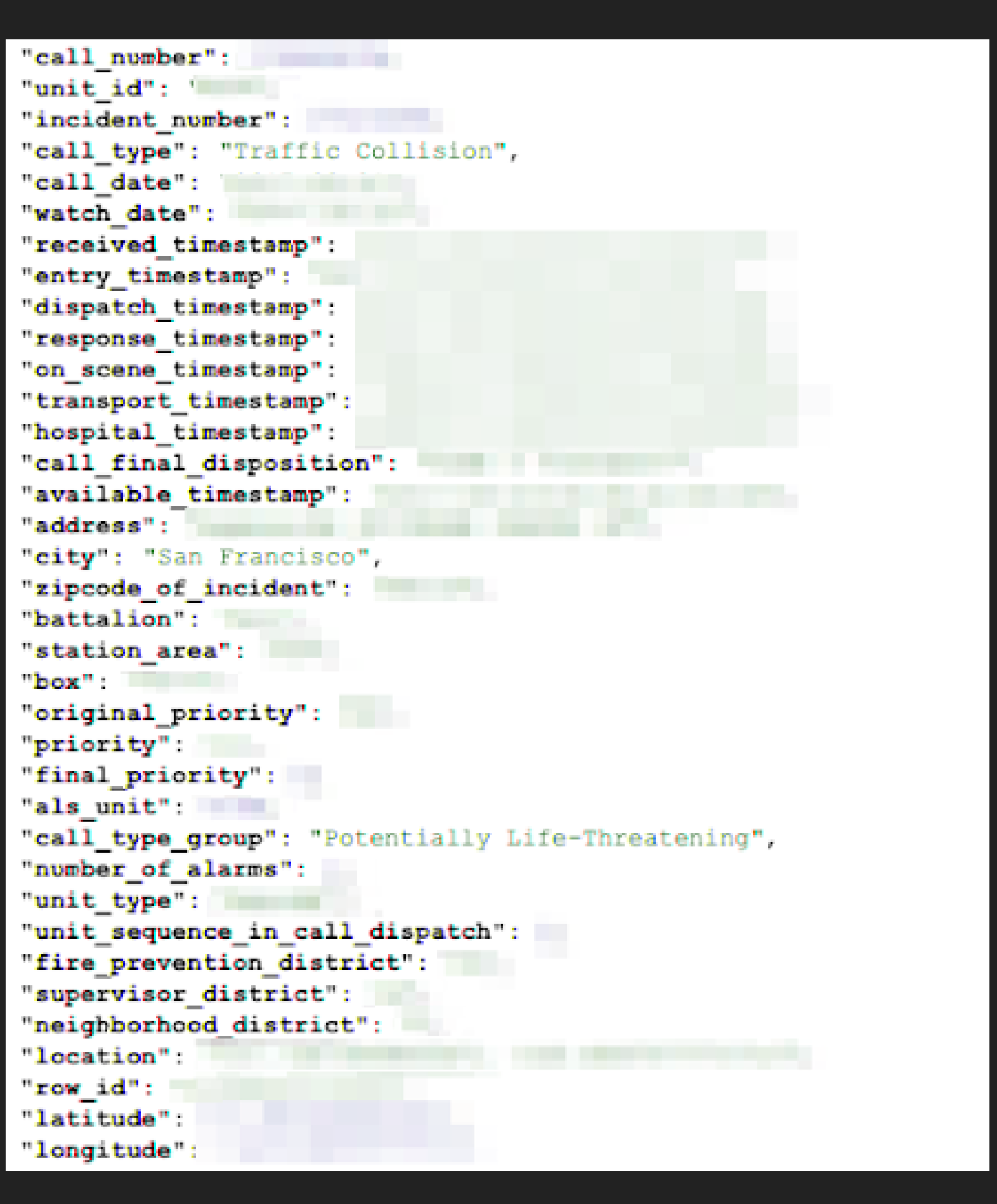
It seems that much of the data on the main folder might have originated from the United States Census Bureau. Certain codes used in the database were either specific to the Bureau or used in the Bureau's classifications.

In addition, the database contained two additional folders that were seemingly unrelated to the mass of personal records we found in the main folder. These folders included the following data:

- **Emergency call logs of a fire department based in the US**
- **A list of some of the 74 bike share stations** that used to belong to a bike share program. The current owner of those bike share stations is Lyft.

While the two smaller folders did not contain any personal information, the call logs from the fire department included **dates, times, locations, and other emergency call metadata dating as far back as 2010**.

Example of leaked fire department call logs:



```
"call_number": [redacted]
"unit_id": '[redacted]
"incident_number": [redacted]
"call_type": "Traffic Collision",
"call_date": '[redacted]
"watch_date": [redacted]
"received_timestamp": [redacted]
"entry_timestamp":
"dispatch_timestamp":
"response_timestamp":
"on_scene_timestamp":
"transport_timestamp":
"hospital_timestamp":
"call_final_disposition": [redacted]
"available_timestamp": [redacted]
"address": [redacted]
"city": "San Francisco",
"zipcode_of_incident": [redacted]
"battalion": [redacted]
"station_area": [redacted]
"box": [redacted]
"original_priority": [redacted]
"priority": [redacted]
"final_priority": [redacted]
"als_unit": [redacted]
"call_type_group": "Potentially Life-Threatening",
"number_of_alarms": [redacted]
"unit_type": [redacted]
"unit_sequence_in_call_dispatch": [redacted]
"fire_prevention_district": [redacted]
"supervisor_district": [redacted]
"neighborhood_district": [redacted]
"location": [redacted]
"row_id": [redacted]
"latitude": [redacted]
"longitude": [redacted]
```

The presence of the mapped bike share station locations and the call logs of the fire department may have indicated that the database might have been either a collection of stolen data or was used by several parties simultaneously, but we were unable to positively confirm this.

Due to how the data in the main folder was structured, however, **our analysts suspect that the database belonged to a data marketing firm or a credit company**. For example, categories and sections were marked as codes in a fashion similar to dictionaries used by data marketers, there were no social security numbers, and all the data profiles we looked at included credit scores.

Who had access?

The database is located in the US and hosted on a Google Cloud server that has been exposed for an unknown period. When we last accessed the database before the wipe, it contained close to 800 gigabytes of data, including the hundreds of millions of records of highly sensitive personal user data that we outlined above. The database itself is still online and accessible but no longer contains any records.

While it's unclear if any malicious actors have accessed the database before the wipe on March 3 or if the data was erased by a blackhat hacker, **anyone who knew where to look could have accessed the data**, without needing any kind of authentication.

What's the impact?

It's difficult to understate the massive effect this data leak can have on hundreds of millions of people in the US. The data exposed by the unidentified party is a virtual gold mine for anyone with a penchant for cybercrime.

Merely selling these records on darknet marketplaces at the below-average asking price of $1 per record would net the seller about $200 million. If utilized by cybercriminals to its full destructive potential, however, this data leak can result in untold billions in damages for defrauded users:

- Scammers can use the names, email addresses, phone numbers, and other private details of the affected users for a wide variety of fraudulent schemes.
- Spammers and phishers can utilize the vast amount of contact details in order to launch targeted attacks against the exposed users on multiple fronts, such as emails and text messages.
- While the database does not contain social security numbers that would let credit card fraudsters engage in outright identity theft, the amount of personal details available in these records is perfect for profiling, impersonation, and other forms of social engineering.

What happened to the data?

After having spent several weeks looking for the owners of this unprotected database, we did not manage to discover who it belonged to before the unidentified party erased all the records and left a link to a website where a dancing pirate urges visitors to fix their security. This means that as of this moment, **the ultimate fate of more than 200 million US user records is unclear**.

In the best case scenario, the mysterious party was an ethical hacker who simply deleted the data because they couldn't identify the owner. In the worst case scenario, however, the data has been copied and will be used by cybercriminals to its full destructive potential. Hopefully, it's the former.

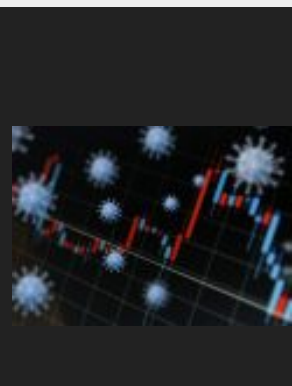
Share 70 Tweet Share

CyberNews Team

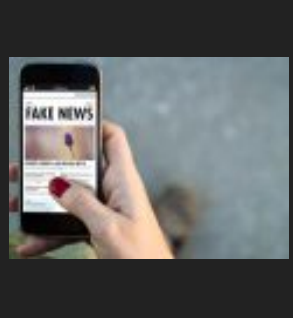
Sometimes, it takes an entire team to bring you a report. The CyberNews Team works diligently to bring you breaking reports of online privacy and security issues, backed by in-depth technical analysis and investigative reporting. You can find us on Twitter anytime.

Related Posts

Mapping the consequences of cyber-physical attacks
MARCH 19, 2020



Corporates face ransomware threat as coronavirus phishing campaigns spread
MARCH 18, 2020



How disinformation and data-driven propaganda is making citizens vulnerable
MARCH 17, 2020

Accenture research highlights the slow pace of progress on cybersecurity
MARCH 13, 2020

Comments 1

Newton Heideman 21 hours ago

Did these retarded database monkeys work for Equifax too?

Reply

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

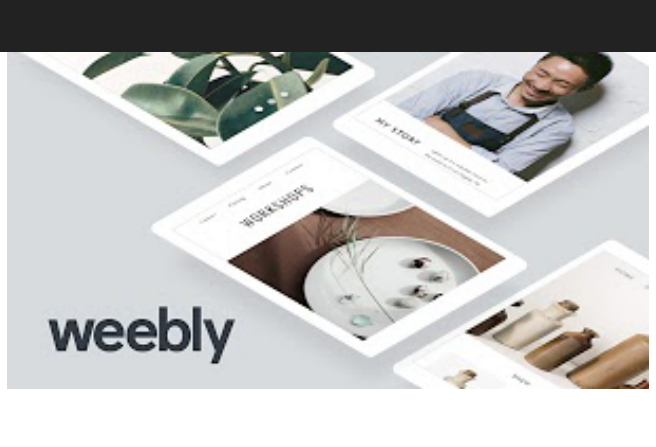
Privacy Policy Agreement *

☐ I agree to the Terms & Conditions and Privacy Policy.

POST COMMENT

Popular News

Report: unidentified database exposes 200 million Americans 01
70 SHARES



Ad
Talk To An Expert With Weebly Customer Service.
www.Weebly.com Visit Site

02 These camera apps with billions of downloads might be stealing your data and infecting you with malware
366 SHARES

03 We found 6 critical PayPal vulnerabilities – and PayPal punished us for it
586 SHARES

04 The ultimate guide to safe and anonymous online payment methods in 2020
0 SHARES

05 Discord privacy tips that you should use in 2020
3 SHARES

Coronavirus is testing the tech sector to its breaking point
MARCH 20, 2020

Report: unidentified database exposes 200 million Americans
MARCH 20, 2020

Mapping the consequences of cyber-physical attacks
MARCH 19, 2020

Corporates face ransomware threat as coronavirus phishing campaigns spread
MARCH 18, 2020

How disinformation and data-driven propaganda is making citizens vulnerable
MARCH 17, 2020

Accenture research highlights the slow pace of progress on cybersecurity
MARCH 13, 2020

Newsletter

Get the most important cybernews to your mail

Subscribe to our mailing list to receives daily updates direct to your inbox!

Your email address SIGN UP

Categories

Editorial Privacy Security
News Resources

About Us

We aim to provide you with the latest tech news, product reviews, and analysis that should guide you through the ever-expanding land of technology.

© 2020 CyberNews - Latest tech news, product reviews, and analyses.